Kasra Ahmadi, Ph.D Candidate.
Work Authorization: U.S. Permanent Residency Process Initiated (Approved I-140 (NIW))
Tampa, FL, 33617 | ahmadi1@usf.edu | 8136142640
https://www.linkedin.com/in/kasra-ahmadii | Portfolio | GitHub| Google Scholar

Summary

Ph.D. candidate in Computer Science with a **3.93 GPA** and a strong background in **Algorithms**, **Cryptography**, and **Machine Learning**. Experienced in conducting high-impact research in **Privacy-preserving AI** and **Post-Quantum Cryptography**. Proven coding skills in Python, C++, and JavaScript, with hands-on work in distributed systems, embedded design, and cloud technologies. Adept at writing production-quality code and optimizing high-performance applications for edge devices.

Education

- **Ph.D. in Computer Science** - University of South Florida, Tampa **-** Jan 2022 to Dec 2025 (Expected).
  Focus: Privacy in ML and Post-Quantum Cryptography | GPA: 3.93
- M.Sc. in Information Technology - Amirkabir University of Technology, Tehran - Sep 2018 to Sep 2021.
  Thesis: Secure file sharing market on Blockchain using smart contracts
- B.Sc. in Computer Science **-** Isfahan University of Technology**,** Isfahan - Sep 2012 to Jul 2017.

Technical Skills

Programming: Python (Proficient), C++ (Intermediate), Java (Intermediate), JavaScript(Proficient),Rust (familiar)
ML: PyTorch, Scikit-learn, Transformers, Flower
Cloud: AWS (Lambda, Glue, S3, DynamoDB), GCP
Databases: SQL, MongoDB
Embedded: Vivado**,** Vitis, ARM, FPGA, HLS, Cortex-M4
Other: Git, Docker, Scrum, Redis, Websocket, API
Soft-skills: Mentorship, Problem-Solving, Communication, Adaptability

Professional Experience

- **Graduate Research Assistant -** University of South Florida, Tampa, FL Jan 2022 - present
  - Developed a privacy-preserving framework combining differential privacy and **federated learning** to fine-tune **LLMs** on edge devices with limited memory.
  - Designed and implemented algorithm-level error detection for **Post Quantum Cryptographic** protocols (Kyber, Dilithium, ECSM) to protect against fault attacks using ARM and FPGA architectures.
  - Built fault-tolerant cryptographic pipeline and benchmarked performance across embedded platforms.
  - Teaching assistant for Cryptography, Operating Systems, and System Design Lab.

- **Software Engineer Intern** - Agwise**,** St.Petersburg, FL May 2024 - Aug 2024
  - **Led** technical team in designing an event-driven architecture using **AWS** services to build a nutrient recommender system for agriculture.
  - Developed **ETL** pipelines with AWS Lambda and Glue to automate lab data ingestion and recommendation delivery.
  - Boosted API and client-side rendering performance by 30% through backend and frontend optimization.

- **Machine Learning Engineer,** Paar Lift**,** Tehran Jan 2019 - Apr 2020
  - Built simulation engine in Python to **optimize** elevator routing using ML models (**Neural Networks** and **Ensemble learning**), reducing passenger wait time by 27%.
  - Designed ETL pipelines using Airflow to process elevator traffic data.
  - Developed real-time data capture using **Raspberry Pi**, CAN Bus, and WebSockets.

Publications & Projects

Machine Learning

- An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Model. **In 2025 IEEE Security and Privacy Workshops (SPW)**. GitHub, Paper.
- **Privacy-Preserved RAG:** Developed and deployed a secure RAG system using LLMs and embedding techniques to enable efficient querying and understanding of a 100MB document corpus. GitHub.

Cryptography & Cybersecurity

- Efficient Error Detection Schemes for ECSM Window Method Benchmarked on FPGAs. ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***. GitHub, Paper.
- Efficient Error Detection Cryptographic Architectures Benchmarked on FPGAs for Montgomery Ladder. ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***. GitHub, Paper.
- PUF-Dilithium/Kyber: Design of a PUF-Based Dilithium/Kyber Architectures Benchmarked on ARM Processors. ***ACM Trans. Embed. Comput. Syst.*** Paper (Dilithium), Paper (Kyber)
- Efficient Algorithm Level Error Detection for Number-Theoretic Transform used for Kyber Assessed on FPGAs and ARM. ***ACM Trans. Embed. Comput. Syst*** *(under-review)* GitHub, Paper.
- Efficient Fault Detection Architectures for Modular Exponentiation Targeting Cryptographic Applications Benchmarked on FPGAs ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems.*** Paper
- **HexGuard Remote Programmer**: Programmed and delivered a QT-based C++ application with a secure server backend with Node.js to remotely program Microchip microcontrollers with authentication and authorization.

Blockchain

- **Smart Contract based Marketplace:** P2P file sharing with IPFS and Ethereum smart contracts. Presented at IEEE AIBThings 2023. GitHub, Paper.

Certifications

- **AWS Certified Solutions Architect** - Associate, View Certification (Dec 2023)
- Deep Neural Networks with PyTorch, View Certificate (Oct 2024)
- Intro to Federated Learning, View Certificate (Oct 2024)
- Artificial Intelligence Privacy and Convenience, View Certificate (Aug 2024)
- Federated Fine-tuning of LLMs with Private Data, View Certificate (Aug 2024)
- ETL and Data Pipelines with Shell, Airflow and Kafka, View Certificate (Jan 2024)
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms, View Certificate (Oct 2023)

Professional Activities

- PhD research funded by National Science Foundation Grant #1801488.
- Peer Reviewer: IEEE TCAS, IEEE VLSI Systems, ACM TECS (18+ manuscripts)
- Recipient of Graduate Research Assistant Scholarship, Muma College of Business, USF.
- Speaker at Great American Teach-In (2023) on AI and emerging technologies.
- Contributed bug fix to Flower federated learning framework.
- Mentor, NSF REU Site: Cryptography and Coding Theory, University of South Florida (Summer 2023)